Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) In a network connectable to a printer and a registration server, a network registration protocol for registering the printer on the network, including the steps of:

installing a secret unique identifier in the printer and in a database of the registration server, before the printer is connected to the network; and,

upon connection of the printer to the network:

causing the printer and the registration server to determine a session key;

transmitting ~~the secret unique identifier~~ from the printer to the registration server a message formed by encrypting, using the session key:

the secret unique identifier;

a public unique identifier; and,

a public key of a public/private key pair;

~~and receiving the identifer in the registration server using a secure transmission over said network, wherein the secret unique identifier is not otherwise transmitted in the clear, when the printer is connected to the network; and~~

authenticating the printer to the registration server by causing the registration server to:

decrypt the message using the session key;

use the public unique identifier to obtain ~~comparing~~ the secret unique identifiers installed in the database;

compare the secret unique identifier installed in the database with the ~~of the registration server and~~ secret unique identifier received in the message; and,

generating and storing in the registration database a certificate containing the public unique identifier and associated public key, the certificate allowing a server to receive a session key from the printer, the session key being encrypted using the private key~~registration server from the printer~~.

2. (Original) The network registration protocol according to claim 1, including the

further step of holding said secret unique identifier in non-volatile memory in said printer, together with a public unique identifier.

3. (Original) The network registration protocol according to claim 2, including the further step of creating a public key together with its paired private key in said printer.

4. (Cancelled)

5. (Cancelled)

6. (Currently amended) The network registration protocol according to claim ~~5~~1, wherein the printer and the registration server determine a session key by having ~~where said secure transmission comprises the further step of~~ said printer obtain~~ing~~ said registration server's certificate, authenticating it with reference to a certificate authority, using a public key-exchange key in said certificate to exchange ~~a~~ the ~~secret~~ session key with the server~~, and then using said secret session key to encrypt said transmission~~.

7. (Cancelled)

8. (Cancelled)

9. (New) A printer for connecting to a network, the printer undergoing registration with a registration server in accordance with a network registration protocol, the printer storing a secret unique identifier installed in the printer and in a database of the registration server, before the printer is connected to the network, wherein upon connection of the printer to the network, the printer undergoes registration by:

determining a session key for communicating with the registration server;

transmitting, to the registration server, a message formed by encrypting, using the session key:

the secret unique identifier;

a public unique identifier; and,

a public key of a public/private key pair;

the registration server being responsive to the message to authenticate the printer by:

decrypting the message using the secret key;

using the public unique identifier to obtain the secret unique identifier installed in the database;

comparing the secret unique identifier installed in the database with the secret unique identifier received in the message; and,

generating and storing in the registration database a certificate containing the public unique identifier and associated public key, the certificate allowing a server to receive a session key from the printer, the session key being encrypted using the private key.

10. (New) A printer according to claim 9, wherein the printer generates the public/private key pair.

11. (New) A printer according to claim 9, wherein the printer communicates securely with servers coupled to the network by:

generating a communication session key;

generating a signature of the communication session key using the private key;

encrypting a message, using a public key of the server, the message including the communication session key and the signature; and,

transmitting the encrypted message to the server, the server being responsive to the message to:

decrypt the encrypted message using a private key of the server;

determine the certificate of the printer;

determine, using the certificate, the public key;

authenticate, using the public key, the signature; and,

use the session key to communicate with the printer in response to a successful authentication.

12. (New) A printer according to claim 9, wherein the printer is adapted to communicate with a sensing device and the network, thereby acting as a relay device to allow the sensing device to communicate via the network.